REMARKS

Applicant has cancelled all device claims 1-6 and 9-11, amended method claims 7 and 8, and added new method claims 12-20. Thus, claims 7-8 and 12-20, which are all method claims, are pending in this application. Applicant has made the amendment in a genuine attempt to address the Examiner's concerns and to place the application in a better condition for allowance or for appeal. It is believed that these amendments do not raise new issues that would require a new search to be conducted. As such, Applicant respectfully requests that these amendments be entered.

The Examiner rejected claims 1-11 under 35 U.S.C. Section 103 as being obvious under Watabe (US Patent No. 4847475) in view of Kelsey (US Patent No. 5907142). Applicant respectfully traverses the rejection.

As briefly discussed in the previous Amendment filed June 23, 2005, the present invention, by way of example only, will now be explained with reference to the figures and specification. As disclosed in paragraphs 5 to 7 and shown in FIG. 5, the invention generally concerns an anti-fraud system that is implemented in a magnetic card reader which is separate from the magnetic card. Conventionally, as a magnetic card 105 is inserted into the card reader 100, a magnetic head 104 reads data recorded on the magnetic stripe 106 of the magnetic card. The data is then saved until it is authorized to be transmitted to a higher level apparatus. In the embodiment shown, the authorization of the data transmission is given when the rear sensor 107 in the card reader 100 senses the front portion of the magnetic card. When the data transmission is authorized, the data is sent to the higher level apparatus and is deleted from the card reader.

One problem associated with such a card reader is that it internally holds the saved data which has been read from the magnetic card 105 until the higher level apparatus receives the data. The holding of the sensitive data within the card reader creates a potential fraud problem because theoretically, the card reader can hold such sensitive data forever if no authorization is ever given to transmit the data to the higher level apparatus. This can happen if, for example, an unauthorized person tricks s the rear sensor 107 such that it fails to detect the positions of the magnetic card 105. In that case, the saved data which has been read off the magnetic stripe is left in the card reader 100. As soon as the cardholder leaves the card reader 100, the unauthorized person with a malicious intent can access the data held in the card reader.

5

To prevent such fraud, the present invention starts a timer, waits for authorization for data transmission to a higher level apparatus, and when the data has not been authorized for transmission and a given time period elapses, the saved data is made unavailable for access. This feature provides the advantage of preventing fraudulent access to sensitive data that has been read off the magnetic card even if sensors in the card reader can be tampered with.

This novel feature is recited in several steps in claim 7 as:

"saving the read data for data transmission to a higher level apparatus"

"waiting for authorization for data transmission of the saved data to the higher level apparatus"

"after starting the timer, when the saved data is not transmitted to the higher level apparatus within the given time period, making the saved data unavailable for reading".

None of the cited references teach or suggest such a novel feature. In the Response to Arguments, the Examiner asserted that Kelsey teaches the recited timer even though the timer in Kelsey is inside the card and not inside the card reader. Applicant respectfully disagrees.

The present invention is directed to an anti-fraud method implemented in a card reader and the data being protected is also inside the card reader. By contrast, the Kelsey system has nothing to do with the card reader. It is strictly concerned with the circuitry and data *inside the card*. Accordingly, Applicant believes that it is inappropriate to equate the data inside the card to data that has already been read out of the card. Specifically, the "read data" in claim 7 refers to data that has already been taken out of the card. Kelsey neither teaches nor discloses protecting data that has already been extracted from the card. Thus, even if it can be combined with Watabe, the combination still does not produce the claimed invention because at best the combination may protect the data inside the card, but does not protect the data inside the card reader which is distinct from the card itself.

Moreover, claim 7 now specifically recites making the read data unavailable "when the saved data is not transmitted to the higher level apparatus within the given time period". Kelsey neither teaches nor suggests protecting the data when the data has not been transmitted to a higher level apparatus.
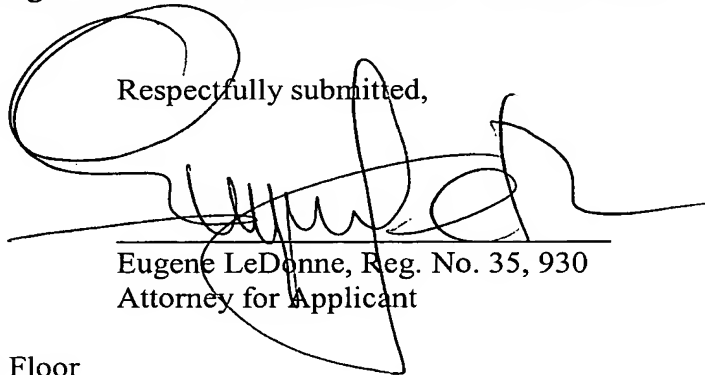
Claim 8 is similar to claim 7 except that the read data is edited before being transmitted to the higher level apparatus. The phrase "the saved and edited data" should be construed to mean data that has been edited and saved. For the similar reasons as discussed above, Applicant submits that claim 8 is also patentable.

Dependent claims 12-17 are also patentable by virtue of their dependency from parent claims 7 and 8.

Applicant has added new independent method claim 18. Claim 18 is drawn along the lines of original claim 7. In addition, it now specifically recites that the timer is located within the card reader, i.e., "starting a *timer in the card reader* for a given time period . . .". This change was made to address the Examiner's concern that the original claims "do[es] not specifically recite where the timer is located". Claim 18 also makes clear that the magnetic card is not a part of the card reader, i.e., "the magnetic card not being a part of the card reader". Accordingly, Applicant respectfully submits that Kelsey directed to only the features inside the card is not applicable to the present invention of claim 18. Dependent claims 19-20 are also patentable by virtue of their dependency from parent claim 18.

Based upon the above amendments and remarks, Applicant respectfully requests reconsideration of this application and its earlier allowance. Should the Examiner feel that a telephone conference with Applicant's attorney would expedite the prosecution of this application, the Examiner is urged to contact him at the number indicated below.

Respectfully submitted,

Eugene LeDonne, Reg. No. 35, 930
Attorney for Applicant

Reed Smith LLP
599 Lexington Avenue, 29th Floor
New York, NY 10022
Tel. (212) 521-5400